PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-229392
(43)Date of publication of application : 25.08.1998

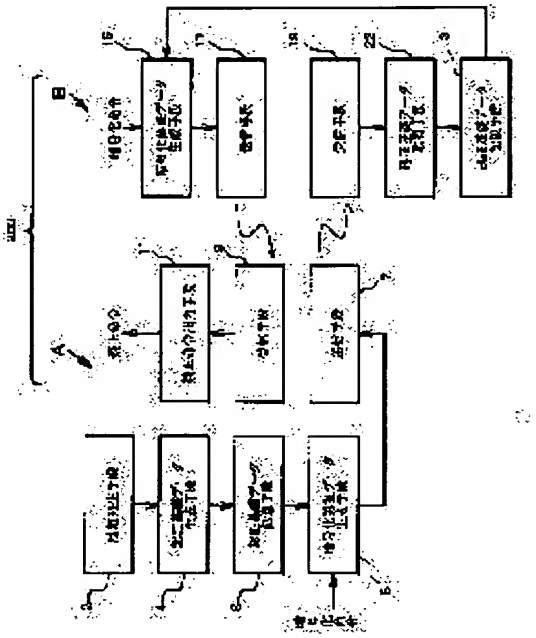
(51)Int.CI. H04L 9/16
G06K 17/00
G09C 1/00
H04L 9/32
H04M 15/00

(21)Application number : 09-029182
(22)Date of filing : 13.02.1997

(71)Applicant : ROHM CO LTD
(72)Inventor : HIKITA JUNICHI
IKUTO YOSHIHIRO
CHIMURA SHIGEMI

(54) AUTHENTICATION SYSTEM AND AUTHENTICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an IC card which is difficult to be used by a person pretending to be a user.
SOLUTION: Ciphering authentication data are generated based on authentication fundamental data, including a random number part by using a ciphering rule, when a ciphering instruction is given by a ciphering authentication data generating means 5. The ciphering rule is varied according to the frequency of a given ciphering instruction. The ciphering authentication data are transmitted by a transmitting means 7. The ciphering authentication data transmitted from a second device B are received by a receiving means 9. A prohibiting instruction output means 11 judges whether or not the ciphering authentication data transmitted from the second device B match the ciphering authentication data generated, when the same frequency of the ciphering instruction is given to the ciphering authentication data-generating means of a first device A and outputs a prohibiting instruction to prohibit the transmission of the subject data to be transmitted, when a judging result is negative.



LEGAL STATUS

[Date of request for examination] 19.11.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－229392

(43)公開日　平成10年(1998)８月25日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/16		Ｈ０４Ｌ　9/00	６４３
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｔ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ａ
Ｈ０４Ｌ　9/32		Ｈ０４Ｍ　15/00	Ｚ
Ｈ０４Ｍ　15/00		Ｈ０４Ｌ　9/00	６７３Ｂ

審査請求　未請求　請求項の数17　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平9－29182

(22)出願日　平成９年(1997)２月13日

(71)出願人　000116024
ローム株式会社
京都府京都市右京区西院溝崎町21番地

(72)発明者　疋田　純一
京都府京都市右京区西院溝崎町21番地　ローム株式会社内

(72)発明者　生藤　義弘
京都府京都市右京区西院溝崎町21番地　ローム株式会社内

(72)発明者　千村　茂美
京都府京都市右京区西院溝崎町21番地　ローム株式会社内

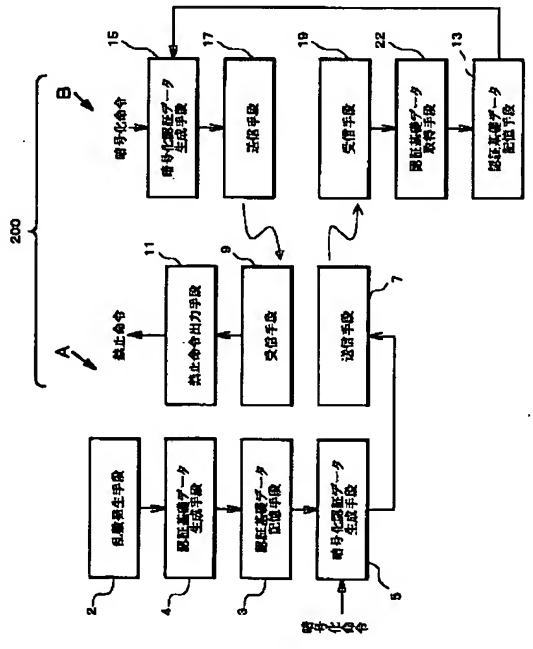
(74)代理人　弁理士　古谷　栄男　（外２名）

(54)【発明の名称】　認証システムおよび認証方法

(57)【要約】

【課題】　なりすましが困難なＩＣカードを提供する。

【解決手段】　暗号化認証データ生成手段５は、暗号化命令が与えられると、暗号化規則を用いて乱数部分を含む認証基礎データに基づいて暗号化認証データを生成する。この暗号化規則は、与えられた暗号化命令回数に応じて変化する。送信手段７は、前記暗号化認証データを送信する。受信手段９は、第２の装置Ｂから送信された暗号化認証データを受信する。禁止命令出力手段１１は、第２の装置Ｂから送信された暗号化認証データが、第１の装置Ａの暗号化認証データ生成手段に同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する。



1

【特許請求の範囲】

【請求項１】第１の装置と第２の装置との間でデータ伝送を行なえるか否かの判断をする認証システムであって、

前記第１の装置および前記第２の装置間で伝送されるデータを暗号化する暗号化規則が単位伝送ごとに変化すること、

を特徴とする認証システム。

【請求項２】第１の装置と第２の装置との間で暗号化した認証データを伝送して、第１の装置と第２の装置との間における伝送対象データの伝送許否を判断する認証システムであって、

前記第１の装置および前記第２の装置間でやりとりされる暗号化された認証データが変化するように、前記認証データを暗号化する暗号化規則が単位伝送ごとに変化すること、

を特徴とする認証システム。

【請求項３】請求項２の認証システムにおいて、

前記第１の装置および前記第２の装置は、ともに、伝送回数に応じて、前記認証データを暗号化する暗号化規則が単位伝送ごとに変化するよう構成されており、

前記第１の装置は、前記第２の装置から送信されたデータが、伝送回数が同じ暗号化規則に基づいて暗号化されたデータと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力すること、

を特徴とする認証システム。

【請求項４】Ａ）第１の装置と第２の装置との間で伝送対象データを伝送する際の認証システムであって、

Ｂ）前記第１の装置は、以下の手段を備え、

b1)認証基礎データを記憶する認証基礎データ記憶手段、

b2)暗号化命令が与えられると、暗号化規則を用いて前記認証基礎データに基づいて暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段、

b3)前記暗号化認証データを送信する送信手段、

b4)前記第２の装置から送信された暗号化認証データを受信する受信手段、

Ｃ）前記第２の装置は、以下の手段を備え、

c1)前記第１の装置から送信された暗号化認証データを受信する受信手段、

c2)前記暗号化認証データ生成手段における暗号化規則に基づいて、前記暗号化認証データから認証基礎データを求める認証基礎データ取得手段、

c3)得られた認証基礎データを記憶する認証基礎データ記憶手段、

c4)前記第１の装置と同じ暗号化規則によって暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段、

c5)前記暗号化認証データを送信する送信手段、

Ｄ）前記第１の装置は、さらに、前記第２の装置から送信された暗号化認証データが、自己の暗号化認証データ生成手段に同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する禁止命令出力手段を備えたこと、

を特徴とする認証システム。

【請求項５】請求項４の認証システムにおいて、

前記暗号化認証データ生成手段は、暗号化された暗号化認証データの多重処理回数を変更することにより、与えられた暗号化命令回数に応じて前記暗号化規則が変化するよう構成されていること、

を特徴とする認証システム。

【請求項６】請求項４または請求項５の認証システムにおいて、

乱数を発生させる乱数発生手段、

予め設定された設定データおよび前記乱数に基づいて、前記認証基礎データを前記認証基礎データ記憶手段に記憶させる認証基礎データ生成手段、

を備えたことを特徴とする認証システム。

【請求項７】請求項４～請求項６のいずれかの認証システムにおいて、

前記送信手段は、前記暗号化認証データを前記伝送対象データに付加させて送信し、

前記受信手段は、前記暗号化認証データが付加された前記伝送対象データを受信し、

前記認証基礎データ取得手段は、前記伝送対象データに付加された前記暗号化認証データを抽出して、認証基礎データを求めること、

を特徴とする認証システム。

【請求項８】請求項４～請求項７のいずれかの認証システムにおいて、

所定時間ごとに、前記暗号化認証データを送信すること、

を特徴とする認証システム。

【請求項９】請求項１～請求項８のいずれかの認証システムにおいて、

前記第１の装置は電話機であり、

前記第２の装置は、前記電話機用のＩＣカードであり、

前記電話機は、単位度数あたりの予め定められた通話可能時間が経過する都度、前記暗号化規則が変化すること、

を特徴とする認証システム。

【請求項１０】Ａ）第２の装置との間で伝送対象データを伝送する際の認証装置であって、

Ｂ）以下の手段を備えたこと、

b1)認証基礎データを記憶する認証基礎データ記憶手

段、
b2)暗号化命令が与えられると、暗号化規則を用いて前記認証基礎データに基づいて暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段
b3)前記暗号化認証データを送信する送信手段、
b4)前記第２の装置から送信された暗号化認証データを受信する受信手段、
b5) 前記第１の装置は、さらに、前記第２の装置から送信された暗号化認証データが、自己の暗号化認証データ生成手段に同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する禁止命令出力手段を備えたこと、
を特徴とする認証装置。
【請求項１１】A) 第１の装置との間で伝送対象データを伝送する際の認証データ作成装置であって、
B) 以下の手段を備えたこと、
1)前記第１の装置から送信された暗号化認証データを受信する受信手段、
2)前記第１の装置の暗号化規則に基づいて、前記暗号化認証データから認証基礎データを求める認証基礎データ取得手段、
3)得られた認証基礎データを記憶する認証基礎データ記憶手段、
4)暗号化命令が与えられると、暗号化規則を用いて前記認証基礎データに基づいて暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段
5)前記暗号化認証データを送信する送信手段、
を特徴とする認証データ作成装置。
【請求項１２】２つの装置間で、伝送対象データを伝送する際の認証方法であって、
与えられた暗号化命令回数に応じて暗号化規則を変化させて、双方側にて認証基礎データに基づいて暗号化認証データを生成し、生成した暗号化認証データをお互いに送受信し、同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データが一致するか否かを少なくとも一方側にて判断して、一致する場合にのみ、前記伝送対象データの伝送を可能とする認証方法において、
前記他方側は、前記一方側から送られてきた暗号化認証データを前記暗号化規則に基づいて復号して、これを前記他方側の認証基礎データとすること、
を特徴とする認証方法。
【請求項１３】請求項１２の認証方法において、
暗号化された暗号化認証データの多重処理回数を変更することにより、与えられた暗号化命令回数に応じて前記暗号化規則を変化させること、
を特徴とする認証方法。

【請求項１４】請求項１３の認証方法において、
前記認証基礎データは、乱数発生させた乱数部分を含んでいること、
を特徴とする認証方法。
【請求項１５】請求項１２～請求項１４のいずれかの認証方法において、
前記暗号化認証データは、前記伝送対象データに付加されて伝送されること、
を特徴とする認証方法。
【請求項１６】請求項１２～請求項１４のいずれかの認証方法において、
所定時間ごとに、前記暗号化認証データを送信すること、
を特徴とする認証方法。
【請求項１７】請求項１２～請求項１４のいずれかの認証方法において、
電話機用と電話機用ＩＣカードとの間の認証方法であって、単位度数あたりの予め定められた通話可能時間が経過する都度、前記認証を行なうこと、
を特徴とする認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、第１の装置と第２の装置との間で伝送対象データを伝送する際の認証に関するものであり、特に、その機密性の向上に関する。
【０００２】
【従来技術】スキー場のリフトや鉄道の自動改札、荷物の自動仕分け等に、ＩＣカードを用いたデータ通信システムが提案されている。
【０００３】図６に、ＩＣカードを用いたデータ通信システムのうち、非接触式ＩＣカードを用いた通信システムの構成を示す。このシステムは、質問器２４０（たとえば、スキー場のリフトのゲート内に搭載される）と非接触ＩＣカード２２０によって構成される。
【０００４】質問器２４０は、質問器側制御部２４８の制御により、発振回路２４９からの高周波搬送波をアンテナ２４１から送り出している。質問器２４０に対して非接触ＩＣカード２２０が接近すると、この高周波搬送波が非接触ＩＣカード２２０のアンテナ２２４によって受信される。電源生成回路２２８は、受信した高周波を直流電力に変換して、他の回路部分に供給する。このようにして、質問器２４０に近づくと、非接触ＩＣカード２２０が動作可能となる。
【０００５】また、質問器２４０から非接触ＩＣカード２２０に対する情報伝達は、前記高周波搬送波を変復調回路２３３において復調することにより行なわれる。カード側制御部２３５は、復調された情報に基づき、メモリ２３７の内容の書き換えや情報返信等の必要な処理を行う。
【０００６】一方、非接触ＩＣカード２２０から質問器

２４０に対しての情報伝達も行われる。非接触ＩＣカード２２０側には、発振回路が設けられていないので、次の様にして、情報送信が行なわれる。質問器２４０の側から無変調の高周波搬送波を送り出しておき、非接触ＩＣカード２２０側にて、変復調回路２３３により、共振回路２２２のインピーダンスを変化させる。質問器２４０は、このインピーダンス変化を、自己側の共振回路２４２のインピーダンス変化として、変復調回路２４６により検出して復調する。制御部２４８は、復調された情報を得て、必要な処理を行う。

【０００７】非接触ＩＣカード２２０が質問器２４０から遠ざかると、電力供給が無くなるので、非接触ＩＣカード２２０の動作は停止する。なお、メモリ２３７は不揮発性メモリであるので、電力供給が無くなっても、記憶された情報は保持される。

【０００８】以上のような非接触ＩＣカード２２０のメモリ２３７に所定の度数を記憶させておき、使用度数に応じてメモリ２３７のデータを書換えることにより、プリペイドカードとして用いることができる。

【０００９】質問器とＩＣカードとの間の通信データは暗号化される。これによって、ＩＣカードの代りとしてコンピュータを接続して、このコンピュータで正規のＩＣカードになりすますこと（以下「なりすまし」という）を防止している。

【００１０】

【発明が解決しようとする課題】しかしながら、このような従来のＩＣカードを用いた通信システムは、次のような問題点があった。上記のように、通信データを暗号化しても、暗号が解読されると、結局、前記なりすましが可能となる。

【００１１】特に、前記ＩＣカードを電話機に用いる場合、通話開始時における認証処理が解読され一旦通話状態となると、何時間でも通話状態とすることが可能となる。

【００１２】この発明は、上記のような問題点を解決し、いわゆるなりすましが困難な認証システムおよび認証方法を提供することを目的とする。

【００１３】さらに、電話機用の認証システムにおいて、通話開始時の認証処理が解読されても、その後、前記なりすましであるか否かの判断をすることができる認証システムを提供することを目的とする。

【００１４】

【課題を解決するための手段】請求項１の認証システムにおいては、第１の装置と第２の装置との間でデータ伝送を行なえるか否かの判断をする認証システムであって、前記第１の装置および前記第２の装置間で伝送されるデータを暗号化する暗号化規則が単位伝送ごとに変化することを特徴とする。

【００１５】請求項２の認証システムにおいては、第１の装置と第２の装置との間で暗号化した認証データを伝

送して、第１の装置と第２の装置との間における伝送対象データの伝送許否を判断する認証システムであって、前記第１の装置および前記第２の装置間でやりとりされる暗号化された認証データが変化するように、前記認証データを暗号化する暗号化規則が単位伝送ごとに変化することを特徴とする。

【００１６】請求項３の認証システムにおいては、前記第１の装置および前記第２の装置は、ともに、伝送回数に応じて、前記認証データを暗号化する暗号化規則が単位伝送ごとに変化するよう構成されており、前記第１の装置は、前記第２の装置から送信されたデータが、伝送回数が同じ暗号化規則に基づいて暗号化されたデータと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力することを特徴とする。

【００１７】請求項４の認証システムにおいては、

Ａ）第１の装置と第２の装置との間で伝送対象データを伝送する際の認証システムであって、

Ｂ）前記第１の装置は、以下の手段を備え、

b1)認証基礎データを記憶する認証基礎データ記憶手段、

b2)暗号化命令が与えられると、暗号化規則を用いて前記認証基礎データに基づいて暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段、

b3)前記暗号化認証データを送信する送信手段、

b4)前記第２の装置から送信された暗号化認証データを受信する受信手段、

Ｃ）前記第２の装置は、以下の手段を備え、

c1)前記第１の装置から送信された暗号化認証データを受信する受信手段、

c2)前記暗号化認証データ生成手段における暗号化規則に基づいて、前記暗号化認証データから認証基礎データを求める認証基礎データ取得手段、

c3)得られた認証基礎データを記憶する認証基礎データ記憶手段、

c4)前記第１の装置と同じ暗号化規則によって暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段、

c5)前記暗号化認証データを送信する送信手段、

Ｄ）前記第１の装置は、さらに、前記第２の装置から送信された暗号化認証データが、自己の暗号化認証データ生成手段に同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する禁止命令出力手段を備えたこと、を特徴とする認証システム。

【００１８】請求項５の認証システムにおいては、前記暗号化認証データ生成手段は、暗号化された暗号化認証

データの多重処理回数を変更することにより、与えられた暗号化命令回数に応じて前記暗号化規則が変化するよう構成されていることを特徴とする。

【００１９】請求項６の認証システムにおいては、乱数を発生させる乱数発生手段、予め設定された設定データおよび前記乱数に基づいて、前記認証基礎データを前記認証基礎データ記憶手段に記憶させる認証基礎データ生成手段を備えたことを特徴とする。

【００２０】請求項７の認証システムにおいては、前記送信手段は、前記暗号化認証データを前記伝送対象データに付加させて送信し、前記受信手段は、前記暗号化認証データが付加された前記伝送対象データを受信し、前記認証基礎データ取得手段は、前記伝送対象データに付加された前記暗号化認証データを抽出して、認証基礎データを求めること、を特徴とする。

【００２１】請求項８の認証システムにおいては、所定時間ごとに、前記暗号化認証データを送信することを特徴とする。

【００２２】請求項９の認証システムにおいては、前記第１の装置は電話機であり、前記第２の装置は、前記電話機用のＩＣカードであり、前記電話機は、単位度数あたりの予め定められた通話可能時間が経過する都度、前記暗号化規則が変化することを特徴とする。

【００２３】請求項１０の認証装置においては、

Ａ）第２の装置との間で伝送対象データを伝送する際の認証装置であって、

Ｂ）以下の手段を備えたこと、

b1)認証基礎データを記憶する認証基礎データ記憶手段、

b2)暗号化命令が与えられると、暗号化規則を用いて前記認証基礎データに基づいて暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段

b3)前記暗号化認証データを送信する送信手段、

b4)前記第２の装置から送信された暗号化認証データを受信する受信手段、

b5) 前記第１の装置は、さらに、前記第２の装置から送信された暗号化認証データが、自己の暗号化認証データ生成手段に同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する禁止命令出力手段を備えたこと、を特徴とする。

【００２４】請求項１１の認証データ作成装置においては、

Ａ）第１の装置との間で伝送対象データを伝送する際の認証データ作成装置であって、

Ｂ）以下の手段を備えたこと、

1)前記第１の装置から送信された暗号化認証データを受信する受信手段、

2)前記第１の装置の暗号化規則に基づいて、前記暗号化認証データから認証基礎データを求める認証基礎データ取得手段、

3)得られた認証基礎データを記憶する認証基礎データ記憶手段、

4)暗号化命令が与えられると、暗号化規則を用いて前記認証基礎データに基づいて暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段

5)前記暗号化認証データを送信する送信手段、を特徴とする。

【００２５】請求項１２の認証方法においては、２つの装置間で、伝送対象データを伝送する際の認証方法であって、与えられた暗号化命令回数に応じて暗号化規則を変化させて、双方側にて認証基礎データに基づいて暗号化認証データを生成し、生成した暗号化認証データをお互いに送受信し、同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データが一致するか否かを少なくとも一方側にて判断して、一致する場合にのみ、前記伝送対象データの伝送を可能とする認証方法において、前記他方側は、前記一方側から送られてきた暗号化認証データを前記暗号化規則に基づいて復号して、これを前記他方側の認証基礎データとすること、を特徴とする。

【００２６】請求項１３の認証方法においては、暗号化された暗号化認証データの多重処理回数を変更することにより、与えられた暗号化命令回数に応じて前記暗号化規則を変化させることを特徴とする。

【００２７】請求項１４の認証方法においては、前記認証基礎データは、乱数発生させた乱数部分を含んでいることを特徴とする。

【００２８】請求項１５の認証方法においては、前記暗号化認証データは、前記伝送対象データに付加されて伝送されることを特徴とする。

【００２９】請求項１６の認証方法においては、所定時間ごとに、前記暗号化認証データを送信することを特徴とする。

【００３０】請求項１７の認証方法においては、電話機用と電話機用ＩＣカードとの間の認証方法であって、単位度数あたりの予め定められた通話可能時間が経過する都度、前記認証を行なうことを特徴とする。

【００３１】

【発明の効果】請求項１の認証システムにおいては、前記第１の装置および前記第２の装置間で伝送されるデータを暗号化する暗号化規則が単位伝送ごとに変化する。したがって、いわゆるなりすましが困難な認証システムを提供することができる。

【００３２】請求項２の認証システムにおいては、前記第１の装置および前記第２の装置間でやりとりされる暗号化された認証データが変化するように、前記認証デー

タを暗号化する暗号化規則が単位伝送ごとに変化する。したがって、いわゆるなりすましが困難な認証システムを提供することができる。

【００３３】請求項３の認証システムにおいては、前記第１の装置は、前記第２の装置から送信されたデータが、伝送回数が同じ暗号化規則に基づいて暗号化されたデータと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する。したがって、第１の装置と前記第２の装置との暗号化処理が異なる場合には、前記第１の装置と前記第２の装置との間の伝送を禁止することができる。また、暗号化規則の特定を伝送回数により行なうので、いわゆるなりすましがより困難となる。

【００３４】請求項４の認証システムにおいては、前記第１の装置は、暗号化命令が与えられると、前記認証基礎データに基づいて与えられた暗号化命令回数に応じた暗号化認証データを生成し、これを送信する。前記第２の装置は、前記第１の装置から送信された暗号化認証データを受信し、前記暗号化認証データ生成手段における暗号化規則に基づいて、前記暗号化認証データから認証基礎データを求め、得られた認証基礎データを記憶する。そして、前記第１の装置と同じく、前記認証基礎データに基づいて与えられた暗号化命令回数に応じた暗号化認証データを生成し、これを送信する。前記第１の装置は、前記第２の装置から送信された暗号化認証データが、自己の暗号化認証データ生成手段に同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する。

【００３５】したがって、前記第１の装置に記憶されている認証基礎データを前記第２の装置に伝送することができる。そして、前記第２の装置における暗号化認証データが異なる生成処理によって行なわれた場合には、前記第１の装置と前記第２の装置との間の伝送を禁止することができる。これにより、いわゆるなりすましが困難な認証システムを提供することができる。

【００３６】請求項５の認証システムにおいては、暗号化された暗号化認証データの多重処理回数を変更することにより、与えられた暗号化命令回数に応じて前記暗号化規則が変化する。したがって、多重処理の回数を制御するだけで暗号化命令回数に応じた暗号化認証データを生成することができる。

【００３７】請求項６の認証システムにおいては、前記認証基礎データ生成手段は、予め設定された設定データおよび前記乱数に基づいて、前記認証基礎データを前記認証基礎データ記憶手段に記憶させる。したがって、前記認証基礎データが固定化されることがない。これにより、いわゆるなりすましがより困難となる。

【００３８】請求項７の認証システムにおいては、前記送信手段は、前記暗号化認証データを前記伝送対象データに付加させて送信し、前記受信手段は、前記暗号化認証データが付加された前記伝送対象データを受信し、前記認証基礎データ取得手段は、前記伝送対象データに付加された前記暗号化認証データを抽出して、認証基礎データを求める。したがって、前記暗号化認証データを伝送するために、前記伝送対象データと別途伝送する必要がない。

【００３９】請求項８の認証システムにおいては、所定時間ごとに、前記暗号化認証データを送信する。したがって、一旦認証したあとも、所定時間ごとに前記認証処理をすることができる。

【００４０】請求項９の認証システムにおいては、前記第１の装置は電話機であり、前記第２の装置は、前記電話機用のＩＣカードであり、前記電話機は、単位度数あたりの予め定められた通話可能時間が経過する都度、前記暗号化規則が変化する。したがって、単位度数あたりの予め定められた通話可能時間経過毎に、前記認証処理が行なわれる。これにより、通話開始時だけでなく、単位度数の通話時間経過ごとに前記照合をすることができる。

【００４１】請求項１０の認証装置においては、暗号化命令が与えられると、前記認証基礎データに基づいて与えられた暗号化命令回数に応じた暗号化認証データを生成し、これを送信する。そして、前記第２の装置から送信された暗号化認証データが、自己の暗号化認証データ生成手段に同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する。したがって、前記第２の装置が行なう生成処理が異なる生成処理である場合には、前記第２の装置との間の伝送を禁止することができる。

【００４２】請求項１１の認証データ作成装置においては、前記第１の装置から送信された暗号化認証データを受信する。そして、暗号化命令が与えられると、前記認証基礎データに基づいて与えられた暗号化命令回数に応じた暗号化認証データを生成し、これを送信する。これにより、前記第２の装置にて、前記第１の装置の認証基礎データを受け取ることができる。また、前記第１の装置にて、前記第２の装置における暗号化認証データを検証することができる。

【００４３】請求項１２の認証方法においては、与えられた暗号化命令回数に応じて暗号化規則を変化させて、双方側にて認証基礎データに基づいて暗号化認証データを生成し、生成した暗号化認証データをお互いに送受信し、同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データが一致するか否かを少なくとも一方側にて判断して、一致する場合にのみ、前記伝送対象データの伝送を可能とする。さらに、前記一方側から送ら

れてきた暗号化認証データを、他方側は前記暗号化規則に基づいて復号して、これを前記他方側の認証基礎データとする。したがって、他方側には、認証基礎データを記憶していなくとも、一方側と他方側にて生成された暗号化認証データが一致しない場合には前記伝送を禁止することができる。

【００４４】請求項１３の認証方法においては、暗号化された暗号化認証データの多重処理回数を変更することにより、与えられた暗号化命令回数に応じて前記暗号化規則を変化させる。したがって、生成回数に応じて異なる暗号化認証データを生成することができる。

【００４５】請求項１４の認証方法においては、前記認証基礎データは、乱数発生させた乱数部分を含んでいる。したがって、前記認証基礎データが固定化されることがない。これにより、いわゆるなりすましがより困難となる。

【００４６】請求項１５の認証方法においては、前記暗号化認証データは、前記伝送対象データに付加されて伝送される。したがって、前記伝送対象データを伝送するだけで前記暗号化認証データを伝送することができる。

【００４７】請求項１６の認証方法においては、所定時間ごとに、前記暗号化認証データを送信する。したがって、一旦認証したあとも、所定時間ごとに前記認証処理をすることができる。

【００４８】請求項１７の認証方法においては、電話機用と電話機用ＩＣカードとの間の認証方法であって、単位度数あたりの予め定められた通話可能時間が経過する都度、前記認証を行なう。したがって、通話開始時だけでなく、通話中にも前記照合をすることができる。

【００４９】

【発明の実施の形態】図面を用いて、本発明にかかる認証システム２００の機能ブロック図について説明する。図１に示す認証システム２００は、第１の装置Ａと第２の装置Ｂとの間で伝送対象データを伝送する際の認証を行なう認証システムである。

【００５０】第１の装置Ａは、乱数発生手段２、認証基礎データ生成手段４、認証基礎データ記憶手段３、暗号化認証データ生成手段５、送信手段７、受信手段９および禁止命令出力手段１１を備えている。乱数発生手段２は乱数を発生させる。認証基礎データ生成手段４は、予め設定された設定データおよび前記乱数に基づいて、前記認証基礎データを生成して、認証基礎データ記憶手段３に記憶させる。

【００５１】暗号化認証データ生成手段５は、暗号化命令が与えられると、暗号化規則を用いて前記認証基礎データに基づいて暗号化認証データを生成する。この暗号化規則は、与えられた暗号化命令回数に応じて変化する。本実施形態においては、暗号化された暗号化認証データの多重処理回数を変更することにより、与えられた暗号化命令回数に応じて前記暗号化規則が変化するようにした。送信手段７は、前記暗号化認証データを送信する。

【００５２】一方、第２の装置Ｂは、受信手段１９、認証基礎データ取得手段２２、認証基礎データ記憶手段１３、暗号化認証データ生成手段１５、および送信手段１７を備えている。

【００５３】受信手段１９は、第１の装置Ａから送信された暗号化認証データを受信する。認証基礎データ取得手段２２は、第１の装置Ａの暗号化認証データ生成手段５における暗号化規則に基づいて、前記暗号化認証データから認証基礎データを求める。認証基礎データ記憶手段１３は、得られた認証基礎データを記憶する。暗号化認証データ生成手段１５は、暗号化認証データ生成手段５と同じ暗号化規則によって暗号化認証データを生成する。なお、第１の装置と同様に、与えられた暗号化命令回数に応じて前記暗号化規則が変化する。送信手段１７は、この暗号化認証データを送信する。

【００５４】第１の装置Ａの受信手段９は、第２の装置Ｂから送信された暗号化認証データを受信する。禁止命令出力手段１１は、第２の装置Ｂから送信された暗号化認証データが、第１の装置Ａの暗号化認証データ生成手段に同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する。

【００５５】したがって、第１の装置Ａに記憶されている認証基礎データを第２の装置Ｂに伝送することができる。そして、第２の装置Ｂにおける暗号化認証データが異なる生成処理によって行なわれた場合には、第１の装置Ａと第２の装置Ｂとの間の伝送を禁止することができる。これにより、いわゆるなりすましが困難な認証システムを提供することができる。

【００５６】つぎに、第１の装置Ａのハードウェア構成について、図２を用いて説明する。

【００５７】第１の装置Ａは、主制御部４１、乱数発生器４３、乱数ラッチ４５、パスワード記憶部４７、認証基礎データラッチ４９、演算器５１、デコーダ５３、ＲＯＭ５５、シフトレジスタ５７、比較用ラッチ５９、比較器６１および伝送回路６３を有する。

【００５８】主制御部４１は、後述するように各部の制御を行なう。乱数発生器４３は、主制御部４１から乱数発生命令が与えられると、６４ビットの乱数を発生させる。乱数ラッチ４５は、乱数発生器４３にて発生した乱数を保持する。

【００５９】パスワード記憶部４７は、３つのパスワードを記憶する。この場合、パスワード１は、６４ビットの第１の装置のハードウェア製造者のパスワードであり、パスワード２は、３２ビットの第１の装置Ａの運用者のパスワードであり、パスワード３は、３２ビットの第１の装置のソフトウェア設計者のパスワードである。

【００６０】認証基礎データラッチ４９は、パスワード記憶部４７および乱数ラッチ４５から与えられた１２８ビットのデータを保持する。本実施形態においては、認証基礎データラッチ４９に保持されるデータが認証基礎データに該当する。

【００６１】比較用ラッチ５９には、初期状態では、１２８ビットの初期値が保持されている。本実施形態においては初期値として、「００・・・・００」（１２８ビット）を保持させた。

【００６２】演算器５１は、認証基礎データラッチ４９と比較用ラッチ５９とに保持されているデータについて所定の演算を行なう演算器である。具体的には各々のデータの排他的論理和演算を行なう。デコーダ５３は、１２８ビットのデータが与えられると、これを１６ビットのデータにデコードする。ＲＯＭ５５は、１６ビットのアドレスについて、１２８ビットのデータ長のデータを記憶しており、１６ビットのデータを所定の１２８ビットのデータにデータ変換する。これにより、暗号化処理がなされる。

【００６３】比較器６１は、シフトレジスタ５７のデータと比較用ラッチ５９のデータを比較して、主制御部４１に比較結果を出力する。伝送回路６３は、第２の装置Ｂとのデータ伝送を行なう。

【００６４】なお、シフトレジスタ５７は、ＲＯＭ５５または比較器６１への入出力は１２８ビットがパラレル処理され、伝送回路６３との入出力は１ビットづつシリアル処理される。

【００６５】つぎに、第２の装置１のハードウェア構成について、図３を用いて説明する。

【００６６】第２の装置Ｂは、主制御部８１、乱数ラッチ８５、パスワード記憶部８７、認証基礎データラッチ８９、演算器９１、デコーダ９３、ＲＯＭ９５、シフトレジスタ９７、比較用ラッチ９９、伝送回路１０３、ＲＯＭ１０５、エンコーダ１０７および乱数デコーダ１０９を有する。

【００６７】乱数ラッチ８５、パスワード記憶部８７、認証基礎データラッチ８９、演算器９１、デコーダ９３、ＲＯＭ９５、シフトレジスタ９７、比較用ラッチ９９、伝送回路１０３については、それぞれ乱数ラッチ４５、パスワード記憶部４７、認証基礎データラッチ４９、演算器５１、デコーダ５３、ＲＯＭ５５、シフトレジスタ５７、比較用ラッチ５９、伝送回路６３と同じであるので説明は省略する。

【００６８】ＲＯＭ１０５は、ＲＯＭ５５とは、逆方向の処理（復号化）を行なうＲＯＭであり、１２８ビットのアドレスについて、１６ビットのデータ長のデータを記憶しており、１２８ビットのデータを所定の１６ビットのデータに復号化する。

【００６９】エンコーダ１０７は、デコーダ５３とは逆の処理を行なう。すなわち、１６ビットのデータが与えられると、これを所定の１２８ビットのデータにエンコードする。乱数デコーダ１０９は、この１２８ビットのデータからパスワード記憶部８７に記憶されている６４ビットのデータを用いて、残り６４ビットのデータを取り出す。取り出された６４ビットのデータは、乱数ラッチ８５に保持される。

【００７０】すなわち、第２の装置Ｂは、第１の装置Ａとほぼ同じ構成であるが、乱数発生器４３および比較器６１を有せず、一方、ＲＯＭ１０５、エンコーダ１０７、乱数デコーダ１０９を有する。

【００７１】つぎに、認証処理について説明する。まず、主制御部４１は、シフトレジスタ５７に、伝送対象のデータの先頭８ビットが与えられると、これを検知し、乱数発生器４３に乱数発生命令を与える。乱数発生器４３はこれを受けて、６４ビットの乱数を発生させる。ここで、この６４ビットの乱数を値ａとする。ここで、乱数発生器４３にて発生した乱数は乱数ラッチ４５にて保持される。

【００７２】認証基礎データラッチ４９には、パスワード記憶部４７および乱数ラッチ４５から与えられた１２８ビットのデータが保持される。

【００７３】ここで、認証基礎データラッチ４９に保持されるデータをデータＡとする。また、比較用ラッチ５９には、初期状態では、初期値「００・・・・００」（１２８ビット）が保持されているので、演算器５１にて排他的論理和演算が行なわれる。デコーダ５３は、１２８ビットのデータを１６ビットのデータにデコードし、ＲＯＭ５５は、与えられた１６ビットのデータを１２８ビットのデータにデータ変換する。シフトレジスタ５７に、この１２８ビットのデータが与えられる。シフトレジスタ５７に与えられるデータをデータＡ’とする。このデータＡ’が伝送対象のデータの先頭に付加されて伝送回路６３から送信される。

【００７４】図４Ａに認証基礎データラッチ４９、比較用ラッチ５９、シフトレジスタ５７に保持されるデータを示す。このように、第１回目の暗号化認証データの送信時には、認証基礎データラッチ４９にデータＡ，比較用ラッチ５９にデータ０，シフトレジスタ５７にデータＡ’が保持される。

【００７５】つぎに、主制御部４１は、比較用ラッチ５９に取込み命令を出力する。比較用ラッチ５９の入力には、ＲＯＭ５５からのデータすなわちデータＡ’が与えられているので、比較用ラッチ５９は取込み命令を受けて、データをＡ’保持する。比較用ラッチ５９にデータＡ’が保持されると、演算器５１、デコーダ５３、ＲＯＭ５５によって、比較用ラッチ５９の入力には、ＲＯＭ５５からのデータすなわちデータ（ＡeorＡ’）’が与えられる。なお、ＡeorＡ’とは、データＡとデータＡ’との排他的論理和演算を表す。主制御部４１は、再度、比較用ラッチ５９に取込み命令を出力する。これに

より、比較用ラッチ５９にはデータ（AeorA’）’が保持される。

【００７６】このように、第１の装置Ａにおいては、図４Ｂに示すように、第２の装置Ｂに送信した後、比較用ラッチ５９に伝送回路６３に与えた暗号化認証データを、さらに暗号化したデータを保持している。

【００７７】一方、図３に示す第２の装置Ｂは、伝送回路１０３で、データＡ’が付加された伝送対象のデータを受信する。データＡ’が付加された伝送対象のデータから先頭の１２８ビットのデータがＲＯＭ１０５に与えられ、１２８ビットのデータを１６ビットのデータにデータ変換する。エンコーダ１０７は、与えられた１６ビットのデータを１２８ビットのデータにエンコードする。乱数デコーダ１０９は１２８ビットのデータから、パスワード記憶部８７に記憶されている６４ビットのデータを用いて、残り６４ビットのデータを取り出す。取り出された６４ビットのデータは、乱数ラッチ８５に保持される。

【００７８】このようにして、第１の装置Ａで発生させた乱数ａを第２の装置Ｂの乱数ラッチ８５に伝送することができる。

【００７９】つぎに、伝送回路１０３の受信信号を受けて、主制御部８１は認証基礎データラッチ８９に取込み命令を与える。これにより、認証基礎データラッチ８９に乱数ラッチ８５とパスワード記憶部８７に保持されたデータが取込まれる。この場合、図５Ａに示すように、シフトレジスタ９７に、データＡ’、認証基礎データラッチ８９にデータＡ、比較用ラッチ９９にデータ０が保持される。

【００８０】つぎに、主制御部８１は、シフトレジスタ９７に伝送対象のデータの先頭８ビットが与えられると、これを検知し、認証基礎データラッチ８９に取込み命令を与える。これにより、認証基礎データラッチ８９には、パスワード記憶部８７および乱数ラッチ８５から与えられた１２８ビットのデータが保持される。

【００８１】ここで、認証基礎データラッチ８９には、第１の装置と同様に、データＡが保持される。なぜなら、乱数ラッチ８５に保持されたデータおよびパスワード記憶部８７に記憶されたパスワードが同じだからである。また、比較用ラッチ９９には、初期状態では、第１の装置Ａと同様に、初期値「００・・・００」（１２８ビット）が保持されている。演算器９１は、認証基礎データラッチ８９と比較用ラッチ９９に保持されたデータの排他的論理和演算を行なう。

【００８２】デコーダ９３は、１２８ビットのデータを１６ビットのデータにデコードし、ＲＯＭ９５は、与えられた１６ビットのデータを１２８ビットのデータにデータ変換する。シフトレジスタ９７に、この１２８ビットのデータが与えられる。この場合、データ（AeorA’）’がシフトレジスタ９７に与えられる。制御部８１から伝送命令が与えられると、このデータ（AeorA’）’が伝送対象のデータの先頭に第２回目の暗号化認証データが付加されて伝送回路１０３から送信される。

【００８３】図５Ｂに、認証基礎データラッチ８９、比較用ラッチ９９、シフトレジスタ９７に保持されるデータを示す。このように、第２の装置の第１回目の暗号化認証データの送信時には、認証基礎データラッチ４９にデータＡ，比較用ラッチ５９にデータＡ’シフトレジスタ９７にデータ（AeorA’）’が保持される。

【００８４】つぎに、主制御部８１は、比較用ラッチ９９に取込み命令を出力する。比較用ラッチ９９の入力には、ＲＯＭ９５からのデータ、すなわちデータ（AeorA’）’が与えられているので、比較用ラッチ９９は取込み命令を受けて、データ（AeorA’）’を保持する。比較用ラッチ９９にデータ（AeorA’）’が保持されると、演算器９１、デコーダ９３、ＲＯＭ９５によって、比較用ラッチ９９の入力には、ＲＯＭ９５からのデータ、すなわちデータ（Aeor（AeorA’）’）’が与えられる。主制御部８１は、再度、比較用ラッチ９９に取込み命令を出力する。これにより、比較用ラッチ９９にはデータ（Aeor（AeorA’）’）’が保持される。

【００８５】このように、第２の装置Ｂにおいても、図５Ｃに示すように、第１の装置に送信した後、比較用ラッチ９９に、演算器９１、デコーダ９３、ＲＯＭ９５によって、暗号化したデータを保持している。これは、以下の様な理由による。本実施形態においては、第１の装置Ａから第２の装置Ｂへ、または、第２の装置Ｂから第１の装置Ａへと照合用データを転送する都度、前記暗号化処理を行なっている。したがって、第１の装置Ａと第２の装置Ｂとでお互いに行なっている処理を一致させる必要があるからである。

【００８６】第１の装置Ａは、伝送回路６３で、データ（AeorA’）’が付加された伝送対象のデータを受信する。データ（AeorA’）’が付加された伝送対象のデータからシフトレジスタ５７に与えられると、主制御部４１は、シフトレジスタ５７に出力命令を与える。これにより、先頭の１２８ビットのデータが、比較器６１に与えられる。また、主制御部４１は、比較器６１に照合命令を与える。これにより、比較器６１は、比較用ラッチ５９に保持されたデータとシフトレジスタ５７から与えられたデータを比較する。この場合、第１の装置Ａと第２の装置Ｂとが正規の装置であるので、比較器６１は一致信号を主制御部４１に与える。もし、第２の装置Ｂがなりすましの装置である場合には、比較用ラッチ５９に保持されたデータとシフトレジスタ５７から与えられたデータが一致しないので、この場合は主制御部４１は、伝送禁止命令を出力する。これにより、なりすましを確実に防止することができる。

【００８７】以後、同様にして、第１の装置Ａからの第３回目の暗号化認証データの送信が行なわれ、第２の装置Ｂは送信された暗号化認証データが比較用ラッチ５９に記憶されたデータと一致するか否かが判断される。

【００８８】このようにして、暗号化認証データを順次変更して送ることにより、確実になりすましを防止することができる。

【００８９】また、本実施形態においては、伝送対象データの先頭に１２８ビットのデータを付加して、伝送しているので、暗号化認証データが付加された伝送対象データとして伝送データを見てみると、伝送対象データも結果的に暗号化されているので、命令（コード）を知られることも防止できる。なお、このように、暗号化認証データを付加して伝送するのではなく、暗号化認証データだけを伝送して、前記照合を行なうようにしてもよい。

【００９０】なお、本実施形態においては、第２の装置から送信された暗号化認証データはそのままとし、比較用ラッチ５９に、演算器５１、デコーダ５３、ＲＯＭ５５によって再度暗号化した暗号化認証データを記憶させることにより、一致しているか否かを判断するようにした。これにより、第１の装置Ａには、演算器５１，デコーダ５３，ＲＯＭ５５の逆の処理を行なう回路が不要となる。

【００９１】しかし、かかる方法に限定されず、第２の装置から送信された暗号化認証データを演算器５１，デコーダ５３，ＲＯＭ５５の逆の処理を行なう回路にて、復号化して比較するようにしてもよい。さらに、第１の装置Ａ側では、演算器５１，デコーダ５３，ＲＯＭ５５の逆の処理全部ではなく、一部だけ行ない、第２の装置から送信された暗号化認証データをこれと一致する処理を行なう様にしてもよい。

【００９２】本実施形態においては、本発明をＩＣカード（第２の装置）とそのリードライタ（第１の装置）に用いた場合について説明したが、第１の装置と第２装置間でデータを伝送させるシステムであれば、ＩＣカード以外のどの様な装置でも用いることができる。

【００９３】また、非接触式ＩＣカードに限らず、接触式ＩＣカードにも適用することができる。

【００９４】なお、本実施形態においては、前回と異なる暗号化データの生成については、入力データをフィードバックすることによりこれを実現するようにしたが、入力データを所定の規則に基づいて、値を替えるようにしてもよい。また入力データを変更することなく、暗号化のアルゴリズムを変更するようにしてもよい。

【００９５】なお、本実施形態においては、伝送対象データの先頭の８ビット分のデータガシフトレジスタに与えられると、前記暗号化認証データを伝送対象データに付加して伝送している。しかし、伝送対象データの伝送とは無関係に、所定時間をタイマで計測して、所定時間ごとに、前記暗号化認証データだけを伝送するようにしてもよい。

【００９６】また、各伝送対象データごとに前記暗号化認証データを変更しているが、複数伝送対象データごとに変更するようにしてもよい。

【００９７】また、８ビットを検出すると、暗号化認証データの生成を行なうようにしているが、これは、上記暗号化認証データの生成処理に要する時間で決定すればよい。

【００９８】また、暗号化認証データおよび伝送対象データのビット長については、これらに限定されるものではない。

【００９９】なお、本実施形態においては、暗号化処理を第１の装置と第２の装置とで、お互いに１回ずつ多重化していくことにより、暗号化命令の回数を伝送することなく、照合する際の暗号化命令の回数を決定している。これにより、どの様にして暗号化されているかを解析しにくくなる。

【０１００】しかし、これに限定されず、暗号化命令の回数を伝送するようにしてもよい。

【０１０１】第１の装置で乱数部分の値を部分的に決定し、第２の装置で残りの部分の値を決定し、これを統合して、乱数ラッチ４５、乱数ラッチ８５に記憶するようにしてもよい。これにより、より機密性を高くすることができる。

【０１０２】なお、一部をソフトウェアで実現するようにしてもよい。

【０１０３】なお、本明細書において、「与えられた暗号化命令回数に応じて前記暗号化規則が変化する」とは、実施形態に示すように、暗号化の多重度を変更することにより、これを実現する場合はもちろん、複数の暗号化規則を記憶しておき、暗号化命令回数に応じて、これを切換えるものも含む。また、暗号化の多重度とは、第１の装置Ａでは、演算器５１、デコーダ５３、ＲＯＭ５５によって暗号化した暗号化処理回数を意味し、第２の装置Ｂでは、演算器９１、デコーダ９３、ＲＯＭ９５によって暗号化した暗号化処理回数に該当する。

【０１０４】また、本発明にかかる認証システムを電話機とそのＩＣカードとの間の認証に用いることもできる。この場合、電話機側の制御部４１には、１度数あたりの予め定められた通話可能時間が経過する都度、伝送対象のデータである度数削除命令が与えられることとなるので、ＲＯＭ５５等による暗号化処理を行ない、伝送回路６３から、ＩＣカードに対して、暗号化認証データを送るようにすればよい。これにより、１度数あたりの予め定められた通話可能時間が経過する都度、前記照合をすることができる。なお、１度数あたりの予め定められた通話可能時間が経過する都度ではなく、数度数を単位度数として予め定められた通話可能時間が経過する都度前記暗号化認証データを送るようにしてもよい。

19　　20

【０１０５】なお、電話機に用いる場合には、ＩＣカードに記憶されている残度数を最初に読み出しておき、この残度数の範囲内であれば通話可能とするとともにＩＣカードとの間では伝送対象データを伝送せずに、通話終了時に残度数をＩＣカード側に送信し、ＩＣカードの残度数を書換えることも考えられる。この場合には、所定時間経過ごとに、前記暗号化認証データだけを送るようにしてもよい。具体的には、タイマで経過時間を計測しておき、所定時間経過すると、制御部４１に暗号化命令を与え、ＲＯＭ５５等による暗号化処理を行なうようにすればよい。

【０１０６】また、本実施形態においては、認証を行なう為の暗号化認証データを伝送対象のデータの先頭に付加して送信し、受信側で暗号化認証データを抽出するようにした。しかしこれに限定されず、伝送対象データを所定の内容としておき、伝送対象のデータを所定の暗号化規則にて暗号化して送信し、受信側にて対応する復号処理を行ない、伝送された伝送対象データが前記所定の内容であるかを判断するようにしてもよい。すなわち、認証データとは、伝送対象データとは別に伝送される場合はもちろん、伝送対象データそれ自体を間接的に認証データとして用いる場合も含む。

【０１０７】また、「暗号化規則が単位伝送ごとに変化する」とは、送信側から受信側に伝送される都度、すなわち、伝送１回毎に暗号化規則が変化する場合はもちろん、所定伝送回数ごとに暗号化規則が変化する場合を含む。

【図面の簡単な説明】

【図１】本発明にかかる本発明にかかる認証システム２００の全体構成図である。

【図２】第１の装置Ａのハードウェア構成を示す図である。

【図３】第２の装置Ｂのハードウェア構成を示す図である。

＊【図４】第１の装置Ａの認証基礎データラッチ、比較用ラッチ、シフトレジスタに保持されるデータの遷移を示す図である。

【図５】第２の装置Ｂの認証基礎データラッチ、比較用ラッチ、シフトレジスタに保持されるデータの遷移を示す図である。

【図６】従来のＩＣカード３００を示す図である。

【符号の説明】

４１・・・・・・主制御部
４３・・・・・・乱数発生器
４５・・・・・・乱数ラッチ
４７・・・・・・パスワード記憶部
４９・・・・・・認証基礎データラッチ
５１・・・・・・演算器
５３・・・・・・デコーダ
５５・・・・・・ＲＯＭ
５７・・・・・・シフトレジスタ
５９・・・・・・比較用ラッチ
６１・・・・・・比較器
６３・・・・・・伝送回路
８１・・・・・・主制御部
８５・・・・・・乱数ラッチ
８７・・・・・・パスワード記憶部
８９・・・・・・認証基礎データラッチ
９１・・・・・・演算器
９３・・・・・・デコーダ
９５・・・・・・ＲＯＭ
９７・・・・・・シフトレジスタ
９９・・・・・・比較用ラッチ
１０３・・・・・伝送回路
１０５・・・・・ＲＯＭ
１０７・・・・・エンコーダ
１０９・・・・・乱数デコーダ

＊

【図４】

A
第1発信時

ラッチ49	A
ラッチ59	O
シフトレジスタ	A'

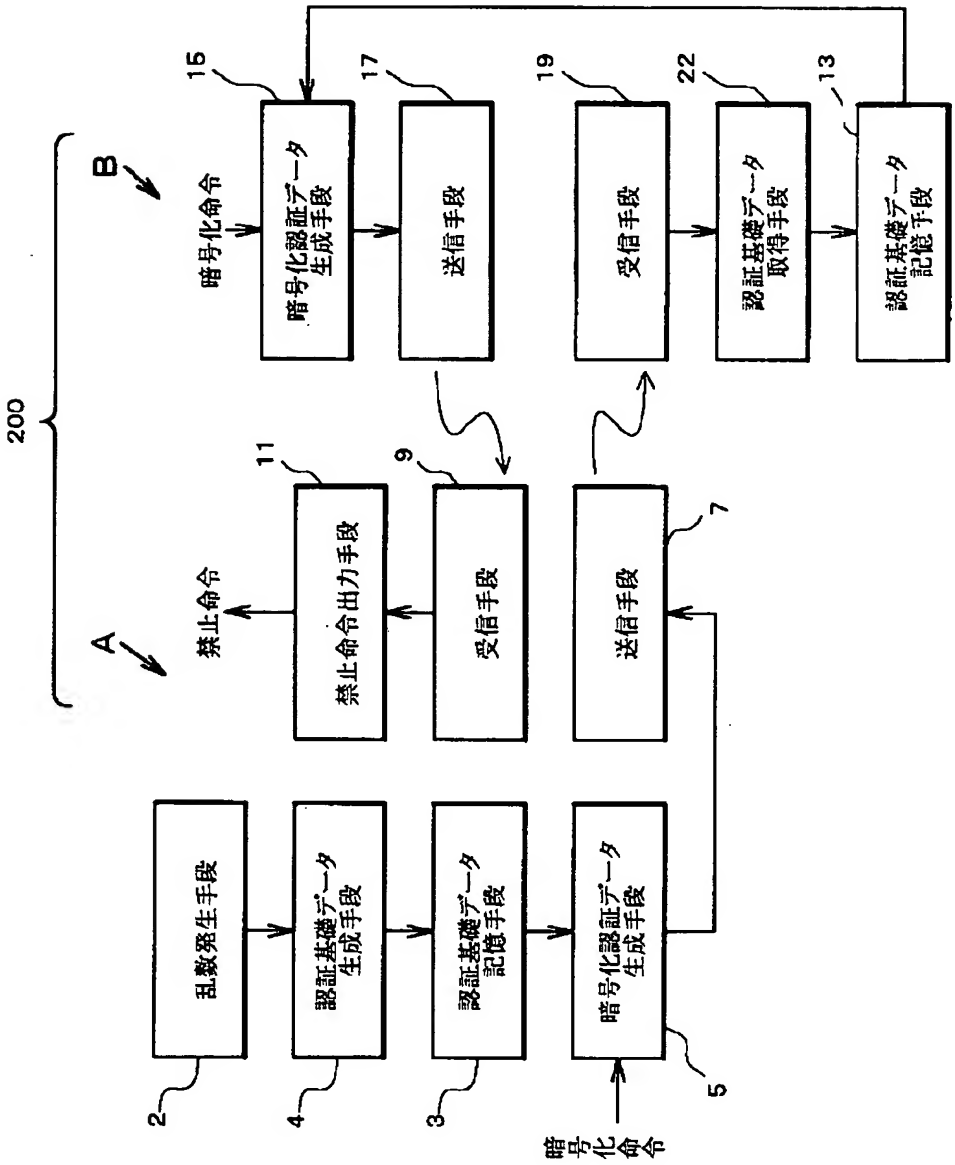
B
準備時

ラッチ49	A
ラッチ59	(AeorA')'
シフトレジスタ	—

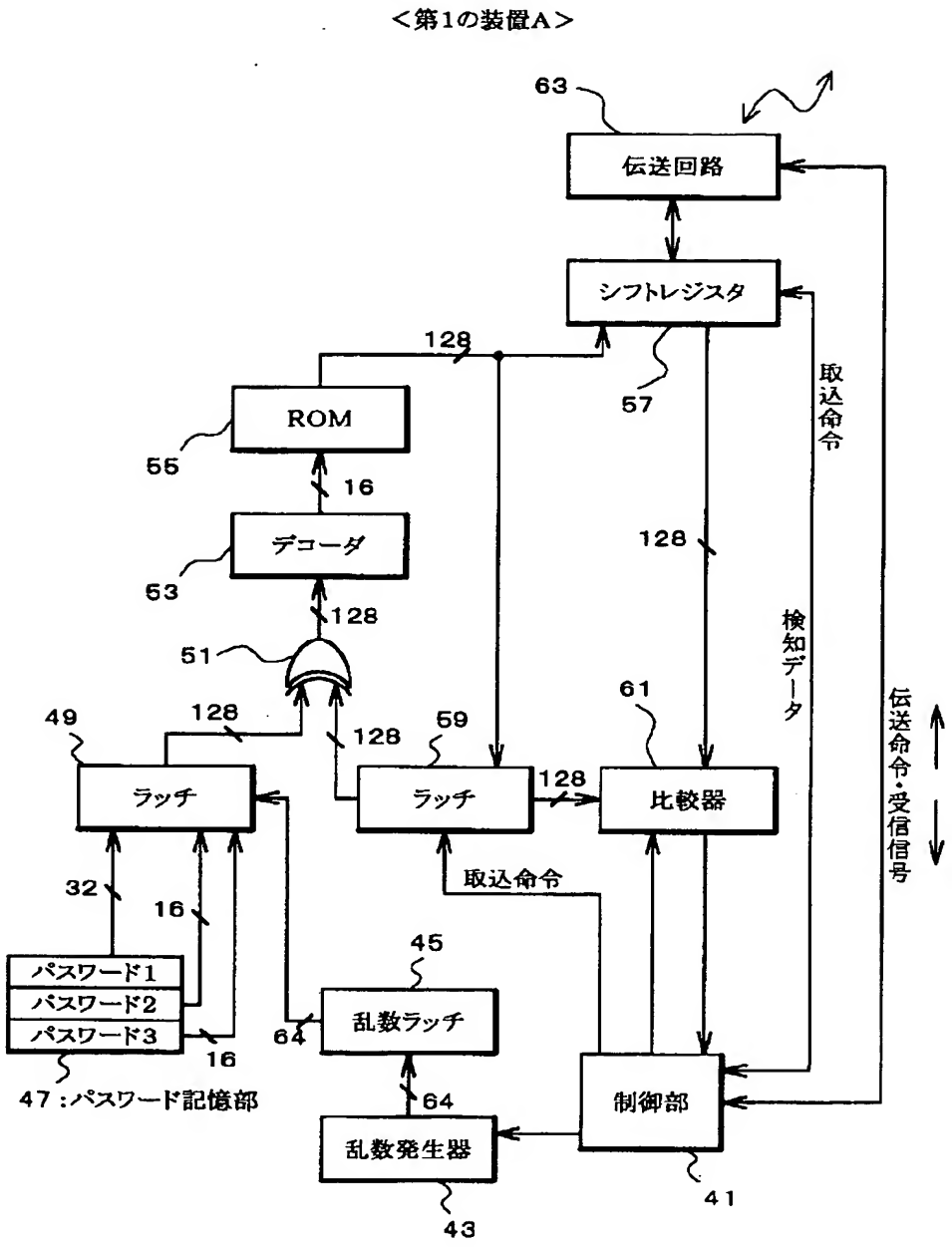
C
受信時

ラッチ49	A
ラッチ59	(AeorA')'
シフトレジスタ	(AeorA')'

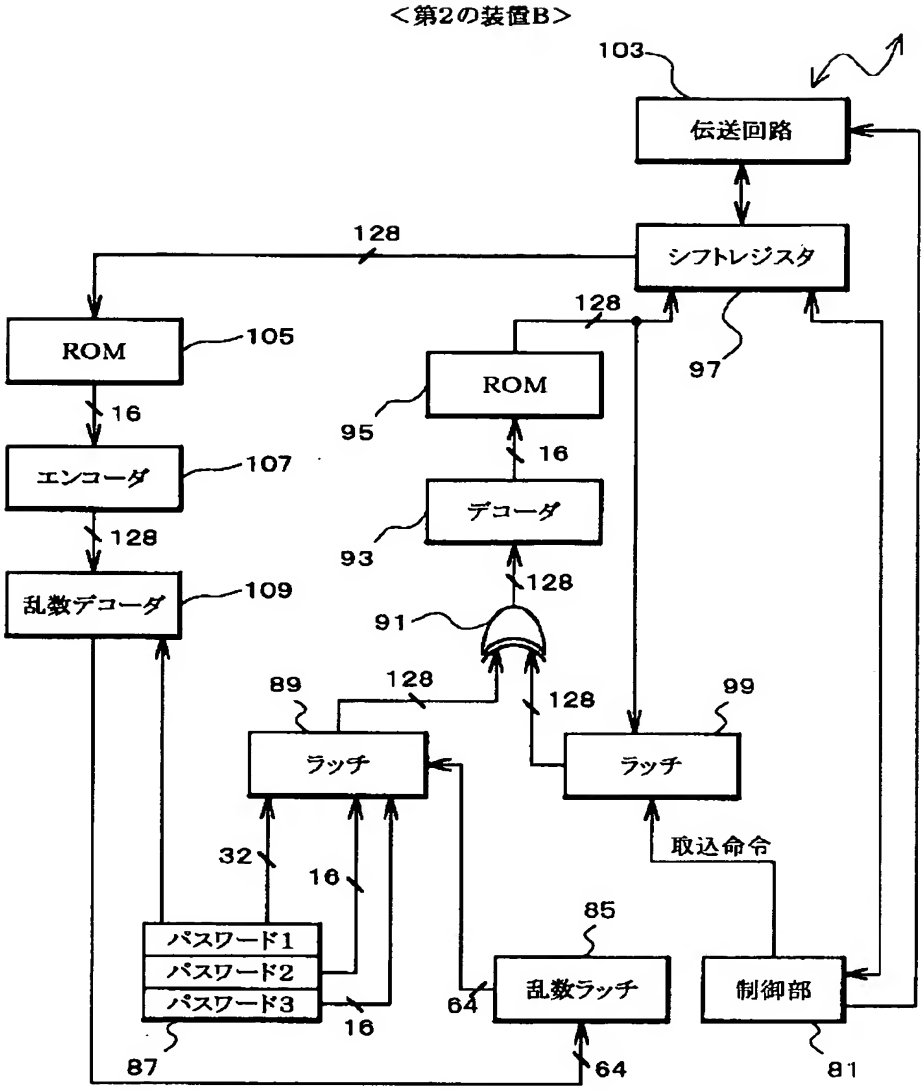
【図１】


200
A
B
乱数発生手段
認証基礎データ生成手段
認証基礎データ記憶手段
暗号化認証データ生成手段
暗号化命令
禁止命令
禁止命令出力手段
受信手段
送信手段
暗号化認証データ生成手段
送信手段
受信手段
認証基礎データ取得手段
認証基礎データ記憶手段
2
4
3
5
11
9
7
15
17
19
22
13

【図２】


＜第1の装置A＞
63
伝送回路
シフトレジスタ
128
57
取込命令
ROM
55
16
デコーダ
53
128
128
検知データ
51
61
伝送命令・受信信号
49
128
128
59
128
ラッチ
ラッチ
比較器
取込命令
32
16
45
パスワード1
パスワード2
パスワード3
乱数ラッチ
64
16
47：パスワード記憶部
64
制御部
乱数発生器
41
43

【図３】


＜第2の装置B＞
103
伝送回路
128
シフトレジスタ
128
97
ROM
105
ROM
95
16
エンコーダ
107
16
デコーダ
93
128
乱数デコーダ
109
128
91
89
128
128
99
ラッチ
ラッチ
取込命令
32
16
85
パスワード1
パスワード2
パスワード3
64
乱数ラッチ
制御部
16
87
64
81

【図５】

A
受信時

ラッチ89	A
ラッチ99	O
シフト レジスタ	A’

B
発信時

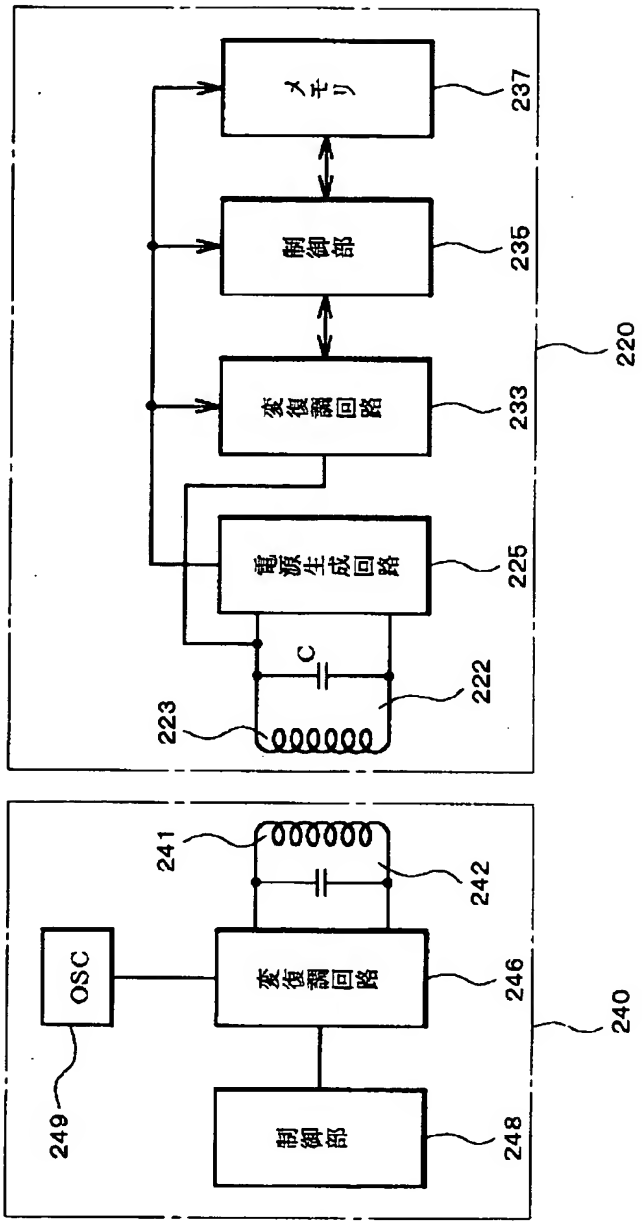
ラッチ89	A
ラッチ99	－
シフト レジスタ	(AeorA')'

C
準備時

ラッチ89	A
ラッチ99	(AeorA')'
シフト レジスタ	－

【図６】

<従来技術>



フロントページの続き

(51) Int. Cl.[6]	識別記号	ＦＩ
		Ｈ０４Ｌ　9/00　　６７３Ｅ